International Journal of Security and Its Applications
Vol. 10, No. 1 (2016), pp.125-138
http://dx.doi.org/10.14257/ijsia.2016.10.1.13

Joint Fingerprinting and Encryption in the DWT Domain for Secure M2M Communication

Conghuan Ye, Zenggang Xiong*, Yaoming Ding, Xueming Zhang and Guangwei Wang and Fang Xu

School of Computer and Information Science, Hubei Engineering University, Xiaogan, Hubei, China
xzg@hbeu.edu.cn

Abstract

Machine-to-machine (M2M) communication is viewed as one of the next frontiers in wireless communications. Because of unguarded communication, new security threats emerge. Considering that multimedia will be widely used in various applications over M2M network, it is very urgent to meet new security requirements for multimedia communication. This paper focuses on a joint fingerprinting and encryption (JFE) scheme in the DWT domain with the purpose of protecting multimedia distribution. A multimedia encryption scheme is first to scramble the multimedia content before distribution, and the fingerprinting scheme is then introduced to provide further protection. The goal of the proposed content distribution scheme is to provide secure content communication and deter the device from illegally redistributing the content. The proposed method, to the best of our knowledge, is the first JFE method in the DWT domain for secure M2M communication. The use of fingerprinting along with encryption can provide a double-layer of protection to digital media. Theory analysis and experimental results show the effectiveness of the proposed scheme.

Keywords: *fingerprinting, M2M, multimedia distribution, multimedia encryption*

1. Introduction

With the fast advance of communication technology and the dramatic penetration of embedded devices, including mobile phones, personal computers, laptops, TVs, speakers, lights, and electronic appliances, M2M (machine-to-machine) has become an indispensable communication component and one of the frontiers for next generation networks. The M2M network technology has become an important field to connect with groups of devices and systems. Aim at enabling interactions between devices ranging from wireless sensors to robots, M2M communications will become a dominant content distribution paradigm in networks. However, it is so difficult to enforce the M2M communication security of wireless networks, since massive smart terminals are expected to be deployed in highly heterogeneous distributed CPS networks.

As the next technology revolution after the computer and Internet, M2M communication often reduces the cost of information acquisition manually, or offers multimedia services based on M2M device. Wireless M2M communications is a form of data transfer that lets machines communicate directly with one another with little or no human interaction or intervention. It covers a wide range of applications, including smart metering, healthcare monitoring, fleet management and tracking, remote security sensing, and on-demand business-charging transactions[1, 2].

* Corresponding Author

ISSN: 1738-9976 IJSIA

Digital content distribution is a predominant service in M2M networks. M2M communication is used for automatic content transmission from remote sources such as digital TV, laptop, Personal Digital Assistant (PDA), smart phone, and MP4 by wire, radio or other means. The consumers have a strong desire to share multimedia content such as Video Surveillance within M2M network. The devices wish to enjoy the content in M2M network easily and conveniently across different M2M devices and locations. It makes multimedia content exchangeable among machinery equipment, people, and the controlling system automaticly. In light of the network architecture and features of M2M communications, it is known that the M2M network plays a decisive role in exchange multimedia content such as audio, video, photos among devices. Such an open architecture and features lead to a number of multimedia security problems during M2M communication. How do consumers determine that M2M system is secure for multimedia content exchange? Most current M2M systems cannot deploy with confidentiality and integrity protocols, leaving their information in the clear for anyone with the right equipment or network access [3]. In fact, the research in security for M2M communications is still in its infancy [4].

In Figure 1, the initializing media device that owns content transmits a request message to content index server, claiming for register of content and admission to setup a new multimedia session to distribute the content to the consumer. In this framework, we assume the existence of a trusted party who audits the participants randomly and punishes the ones who deviate from the legal behavior. The request message contains the basic information of the content and the receivers. Upon receiving the request message, the content index server will send out an inquiry message to the media processing server for content protection and asking for distribution of the content. The content distribution is based on multicast transmissions. Multicast transmissions are efficient by creating a multicast tree, in which, the content provider is the root of the tree, and the receivers are the other nodes in the tree.

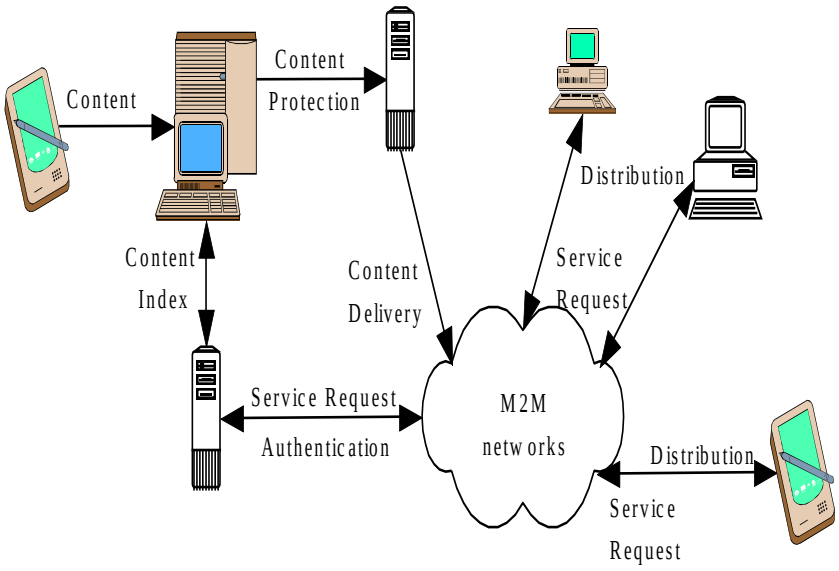

Figure 1. Framework of M2M Communication

In this paper, a novel secure multimedia content distribution using encryption and fingerprinting based on DWT aims at efficiently and effectively deterring the illegal access and redistribution the content in M2M networks. Base on the security demand of M2M communication, the section briefly introduces the framework of secure multimedia sharing in M2M networks. Multimedia content protection is somehow

different from traditional data encryption due to some inherent features of multimedia such as bulk data capacity, so security schemes could not overburden networks or reduce the received quality. An elementary framework of secure content distribution is shown in Figure 1.

In this paper, we propose a DWT based **JFE** scheme for secure multimedia content distribution scheme in M2M network. According to our best knowledge, there has been no report yet on the implantation of DWT transform for secure M2M communication with fingerprinting and encryption. This paper addresses the issue of protecting media distribution using fingerprinting/encryption in DWT domain. First, we describe image preprocessing and wavelet decomposition. Then, we propose a fingerprinting/encryption method in DWT domain. Finally, contents protected are distributed via Hybrid Multicast-Unicast. The remainder of the paper is organized as follows. Section 2 describes the background and related works. In Section 3, the proposed scheme is introduced. Then, the experimental results will be given in Section 4. Section 5 concludes the work of the paper.

2. Related Works

M2M network has been regarded as the next wave of information technology revolution [5] , where the information on the Internet are generated and consumed by machines to achieve ubiquitous intelligence. Nowadays, M2M has become an indispensable component for next generation networks, *e.g*. Internet of Things (IoT) [6]. As M2M networks are interoperable networks, the data travels from one type of networks to another. M2M systems shall protect the privacy of the device and the data. When data gets exchanged, it shall be confidential. Data integrity solutions should guarantee that an adversary cannot modify data in the transaction without the system detecting the change. The problem of data integrity has been extensively studied in all traditional computing and communication systems and some preliminary results exist for sensor networks [7]. The appropriate encryption algorithm shall be applied to ensure the confidentiality of the data. Data confidentiality and integrity, authentication, authorization, treat and virus attack protection, a trusted and secure environment, and secure software upgrades are important security management features for M2M systems [8].

Home M2M communications may expose them to a number of potential attacks such as physical attacks, compromise of credentials, configuration attacks, and core network attacks [7]. In [9], these security vulnerabilities are described in the following categories: Compromise of Credentials, Configuration Attacks, Attacks on the Core Network, Device Data and Identity Privacy Attack. While security is generally perceived as an important constituent of communication systems, the paper [10] offers a viable security-communication trade-off particularly tailored to smart grids. In [11], the authors considered mobile network security elements will become a part of the overall suite of security solutions for M2M as well. Considering the large number of M2M terminals deployed in highly distributed networks in both cellular and Ad Hoc manner, the security issue becomes critical since network operators do not want the hackers to break into the services. A possible solution might be content encryption. An example is to use symmetric architecture, where the machine and the peer share the key–stored in the SIM-to encrypt or decrypt the message [12]. M2M communication security plays a significant role in all fields, especially those related to confidential business.

When video sensors are introduced in M2M systems, intelligent surveillance camera networks and intelligent transportation systems will emerge. In those systems, distributed video sensors/cameras capture video sequences and communicate with the aggregation nodes. The video data are then analyzed and processed on the

aggregation nodes or by the cloud servers [13]. The proliferation of data exchange on the M2M network presents a challenge in the field of multimedia security, as the unauthorized duplication and redistribution of multimedia content become easier. The data could use security mechanisms to enforce confidentiality and integrity. Unfortunately, cost and developmental limitations make this design choice difficult, too [3]. However, the traditional cryptographic techniques can not deter this behavior. Improper use of data and contextual information may cause serious information leakage and provide inaccurate feedback controls [6].

To defend against the security threats and establish a secure M2M communications environment, a suite of security mechanisms are desirable, which should achieve the following requirements: confidentiality, integrity, authentication, non-repudiation, access control, availability, and privacy. In general, these security requirements in M2M communications can be achieved by cryptographic techniques. However, most security mechanisms only efficiently defend against external attacks. Once M2M nodes are compromised and launch some internal attacks such as content redistribution in M2M communications, more sophisticated security mechanisms are needed. Concerned about the consequences of piracy of data, owners are interested in digital rights management (DRM) systems which can protect their rights of digital content [14].

In order to protect multimedia content from illegal use, there are many measures to protect the copyright of owners, such as encryption, copy detection, and digital watermarking *etc*. as Figure 2 shows. Encryption may ensure secure multimedia transmission through communication networks and prevent an unauthorized access. In [15, 16], Multimedia content scrambling algorithms based on partial encryption are proposed. However, once devices receive and decrypt the data, the multimedia content could be copied at their option[17]. In the end, although encryption can provide multimedia content with the desired security during transmission, once a piece of digital content is decrypted, the dishonest customer can redistribute it arbitrarily[18]. In order to deter piracy, Chin-Ling Chen *et al*. [19] proposed a verifiable and traceable secondhand digital media market protocol with encryption and watermarking to trace traitor efficiently.

To maintain acceptable performance, a security strategy must be aware of multimedia-specific needs and not severely detriment metrics such as perceptual quality. Because steganography, multimedia encryption and copy detection realize different security functionalities, they can be combined together to protect both the confidentiality and the identification. Encryption obscures the content from all except the intended recipient. Steganography permit content to be broadcast and viewed without requiring decryption keys, but may include additional information (either overt or covert) for tracking the origin of the media. Copy detection develops automated content authentication procedures to identify the original and modified copies of a multimedia content among a large amount of multimedia data for the purposes of content protection. Steganography, encryption, and copy detecting are broad classes of techniques that can be used as part of communication security solution. The content authentication scheme is shown in Figure 2

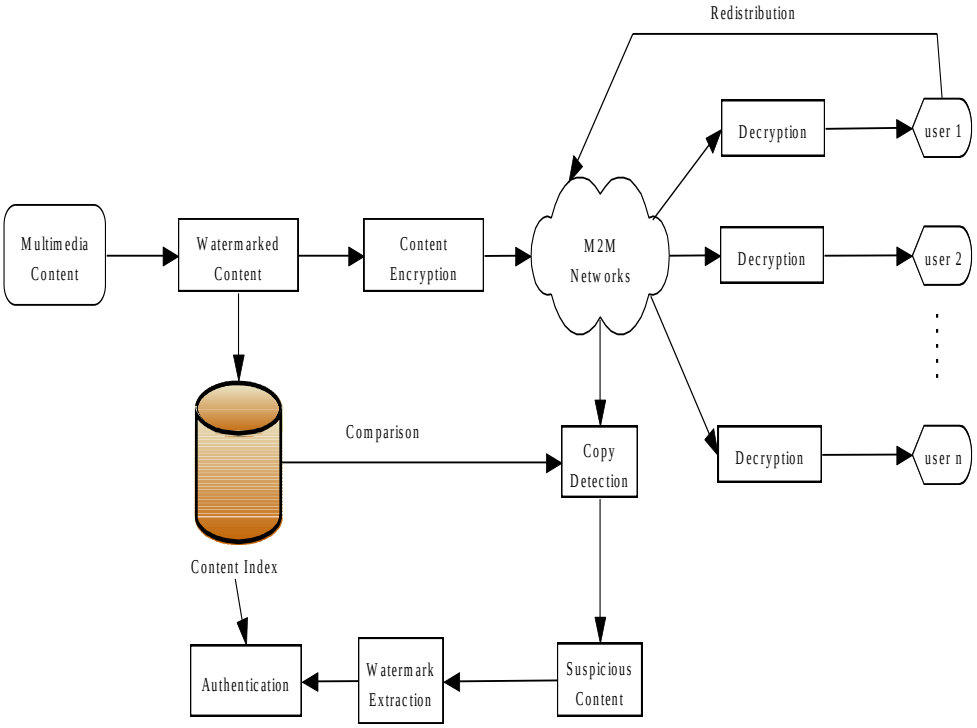

Figure 2. Multimedia Content Distribution and Copyright Authentication Scheme

Nowadays, on one hand, multimedia content is used more and more throughout our daily life because of advance of M2M communication. The distribution of multimedia content will become one of the most widely used applications on the M2M networks. On the other hand, M2M networks devices wish to access any kind of content from any M2M device they have available. Media devices that contain resources should preprocess their multimedia resources to protect privacy. In other words, the media device should manage, control, process and render multimedia content before the content is transmitted from the device and presented to the M2M network.

3. The Proposed Method

Digital watermarking is viewed as a viable solution serving as the final defensive line of content authentication to compensate the possible deficiency of the content protection. However this scheme cannot authenticate the one who redistributed the content. To be more specific, the ID information about the original recipient can be embedded into the multimedia content and, once an illegal copy is found, ID information, namely digital fingerprint, can track the redistribution of digital multimedia to deter the malicious devices from spreading the decrypted content. As a prominent solution, fingerprinting is developed to deter redistribution by embedding a unique serial number into each distributed copy before multimedia content is distributed to devices through M2M communication. If a pirated content is found somewhere by the content distribution sever, then the server extracts the embedded fingerprint information and detects the device who distributed it illegally by analyzing the fingerprint. The concept of traitor tracing was coined in as a method to discourage piracy. Traitor tracing schemes are useful in scenarios where the distributed content may only be accessible to authorized devices, like decrypting messages, and distribution of content.

3.1. Preprocessing

In M2M system with a large number of M2M devices, there may be some of devices which cannot receive high resolution original image because of small memory capacity. Therefore, the high definition image must be preprocessed to meet the memory capacity.

In this paper, it is assumed that there is a valuable high resolution original image with high resolution $M_G \times N_G$. Suppose the original image is represented initially by the array $G_{original}$ which contains N_G columns and M_G rows of pixels. Each pixel represents the light intensity at the corresponding image point by an integer I between 0 and $K-1$.This original image is preprocessed to get an image with resolution $M_G' \times N_G'$ according to the request of device i.

The cropped images are finally reduced or low-pass filtered to get device-specific images with resolution $M^{(i)}{}_G' \times N^{(i)}{}_G'$, where subscript i denote the index of the i-th device. Each value within reduced image is computed as a weighted average of values in original high resolution image within a 3-by-3 window. The averaging process is performed by the function SUBSAMPLE.

$$G_{subsample}=SUBSAMPLE(G_{original}) \quad (1)$$

Which means, for $G_{subsample,}$ and nodes $i, j, 0 \leq i < N_G', 0 \leq j < M_G'$

$$G_{subsample}=\sum_{m=-1}^{1}\sum_{n=-1}^{1} w(m,n)G_{original}\ (2i+m, 2j+n) \quad (2)$$

Where $w(m, n)$ represents the 3-by-3 window. According to the request of device, the reduced image $G_{subsample}$ is reduced by $M_G'/M_G \times N_G'/N_G$ in two dimensions from original image to device-specific image. In this paper, the values of M_G' and N_G' could change to meet the need of devices. The proposed preprocessing scheme can generate device-specific images with different resolution no more than the original resolution. Thus, after being preprocessed, each image to be encrypted and fingerprinted is not perceptual.

3.2. Appropriate Wavelet and Decomposition Levels

The wavelet transform is considered to be a hierarchical subband system, with a filter bank composed of a decomposition filter, a reconstruction filter. In DWT transformation an image is first decomposed into four parts of high, middle, and low frequencies (*i.e.*, *LL*, *LH*, *HL*, *HH* sub-bands) the fingerprints will be embedded into all the wavelet coefficients of *LH* and *HL* subbands. Finally, we divide the coefficients into two parts, the base content and the supplementary content. The base content then will be encrypted via permutation and diffusion and will be freely distributed through multicast M2M communication, while the supplementary content carry the embedded unique fingerprint for each device and be distributed using the traditional server–client mode in M2M network.

Thus, it resolves the conflict of traitor tracing and free sharing. However, this solution requires the fingerprint not only to be small enough to alleviate the load of the server but also to keep two other tradeoffs: robustness and invisibility.

Since the fingerprinted content will be distributed from the central server to all the clients, it should be designed to have enough size to hide more fingerprint information. Thus, the load of the server can be alleviated to some extent. One possible approach to derive an appropriate size of fingerprinted content is to decompose the original image with DWT technology adaptively.

The fingerprinting method employs wavelet transform to model the middle-frequency feature of the image. After the preprocessing, we transform the device-

specific image with DWT technology. We employ 3-level decomposition. In wavelet transform, an image is split into one approximation (also called *LL* subband) and three details in horizontal, vertical, and diagonal directions which are named (or coefficients in *LH* subband), (coefficients in *HL* subband), and (coefficients in *HH* subband). The *LL* subband is then itself split into a second-level approximation and details, and the process is repeated.

For a *J*-level decomposition, the approximation and the details are described in Equation . (3)

$$\begin{aligned} w_{ll}(J) &= < G_{subsample} \cdot LL_J >, \\ w_{lh}(j) &= < G_{subsample} \cdot LH_j >, j = 1, \ldots, J \\ w_{hl}(j) &= < G_{subsample} \cdot HL_j >, j = 1, \ldots, J \\ w_{hh}(j) &= < G_{subsample} \cdot HH_j >, j = 1, \ldots, J \end{aligned} \quad (3)$$

Where $G_{subsample}$ represents the device-specific image and LL_j, LH_j, HL_j, and HH_j are wavelet subband. After decomposition, the coefficients of all *LH*-level and *HL*-level subbands are used to embed fingerprint related device. In this paper, we consider orthogonal fingerprint embedding, where fingerprints assigned to different devices are orthogonal to each other and have the same energy.

3.3. Content Encryption

The Arnold map for encryption can be described as follows

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & 1+ab \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod H \quad (4)$$

Where $x_n, y_n \in (0,1)$ are the states of the chaotic system, a and b are positive integers selected from the discrete set {1,…, *H*-1 }.

For the base content, the encryption process is as follows:

Step1: Perform the content encryption by coefficient permutation using an Arnold chaotic map. For each coefficient, use Arnold map to calculate the new position. After each coefficient is relocated to a new position, the permuted content is generated.

Step2: Diffusion processes can protect content further. Use Arnold map to generate two random sequences, one for the base content and the other is produced for diffusing the supplementary content. The processed content is encrypted to superpose the permuted content. The opponent cannot find any useful clues between the decrypted content and the encrypted and so cannot break the cryptosystem even after they spend a lot of time and effort.

For the supplementary content, the encryption and fingerprinting process is as follows:

Step1: Permute the content encryption by coefficient permutation using an Arnold chaotic map. For each coefficient, use Arnold map to calculate the new position. After each coefficient is relocated to a new position, the permuted content is generated.

Step2: To trace the illegal redistribution, fingerprinting processes can be applied to enhance the protection of the decrypted content. The details about fingerprints embedding and detection will be presented in the next section.

3.4. Fingerprints Embedding and Detection

Digital fingerprinting is a technique for identifying devices which use multimedia content for unintended purposes, such as redistribution. An owner of digital work, who sells the work, wishes to protect his/her copyright and discourage illegal redistribution of his/her products. To this end, he uses watermarking technology to embed a unique watermark (fingerprint) to each copy of the work before it is

delivered.

We assume the total number of devices in multimedia fingerprinting system is M. For the digital media represented by a vector X, and for every device who want to receive the content, the owner generates a sole fingerprint for the device. The fingerprint is embedded into digital media. The watermarked media is delivered to the device. This makes each copy unique and therefore if a dishonest device illegally redistributes his copy, he can be unambiguously identified by traitor tracing scheme. Digital fingerprinting system could realize traitor tracing as Figure 4 shows. Once a pirated copy is detected, the owner extracts the fingerprint of the pirated copy and carries out traitor tracing algorithms to identify the colluders.

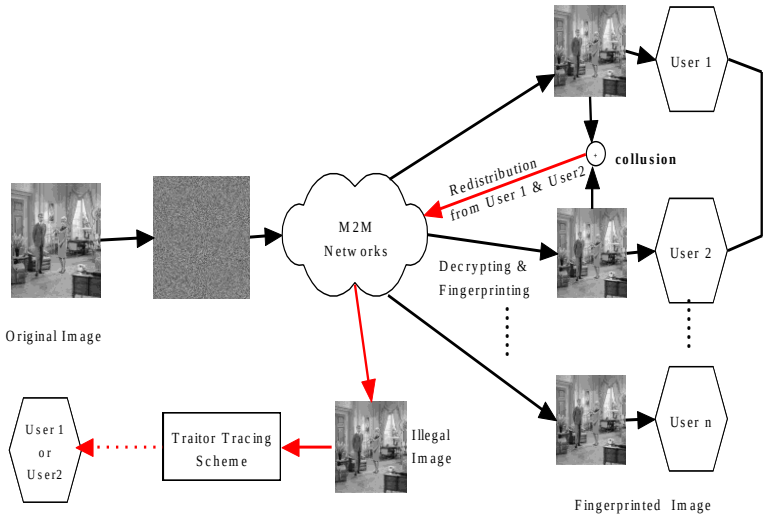

Figure 3. Fingerprinting Scheme for Multimedia Content Protection

In this paper, we focus on blind watermarking to embed fingerprints because the watermark is detected without reference to the original once a pirated image was found. The pirated image could be a colluded copy of original image. When devices come together with a total of K_c differently fingerprinted copies of the same multimedia content, these devices can simply linearly combine the K_c signals to produce a colluded version. Average collusion attack, which belongs to linear collusion, is a cost-effective attack against multimedia fingerprinting. To simplify the description of embedding method, we only discuss how it works on the preprocessed images as well as embedding of a unique fingerprint.

Suppose N_c and N_u are two sets in which there are vectors orthogonal to each other. The vectors, which are regarded as community code and inner fingerprint code, in the two sets are subject to Gaussian distribution. We choose the robust coefficients in all *LH*- level and *HL*-level subbands to combine a vector, $X_c=(x_1, x_2, \ldots, x_{|Nc|})$, as host signals to imbed community code, where N*c* is the length of fingerprint, the hiding scheme is as follow:

$$y_j^{(i)} = q_{x_j} = round\left(\frac{x_j + d_i^{(j)}}{\Delta}\right) \times \Delta \quad (5)$$

where x_j is a vector which denotes the codeward with length $|N_c|$, $i, j = 1, \ldots, |Nc|$, round is an operation of *Floor and Ceiling*, and Δ is a constant. Then, all y_j $(j = 1, \ldots, |Nc|)$, which assigned to devices.

From Figure 5, we also know that the fingerprinting method has a perfect vision effect under allowance of human sight.

Since only the owner keeps the mapping between the fingerprint and the device, as long as the owner successfully tracks back the fingerprint for a suspect multimedia, for example, the pirate device or traitor can be revealed. In this case, to identify the embedded fingerprint, the multimedia producer needs to decompose the fingerprinted image into level 3 using the wavelet technique so that the coefficients of all 3rd-level subbands are obtained. The $|Nc|$ coefficients, which compose a long vector z, are extracted. By deducting, the difference is as follow:

$$T_k = \left\| z - y_k \right\|^2 \quad , \text{k=1, … , |Nu|} \tag{7}$$

Here, the least T_k, which is related to device k, determines who the traitor is

4. Experiment Results and Analysis

In this section, some experimental results are demonstrated to show the effectiveness of the proposed JFE scheme. To demonstrate the security and efficiency of our algorithm, we use some gray scale images as the original test images.

4.1. Perceptual Security

Generally, the encrypted image should be unintelligible for confidentiality. In the proposed scheme, the image is encrypted by permutation via chaotic map first. Furthermore, use another chaotic map to superimpose a random sequence to the permuted coefficients. The visual impact of the proposed encryption scheme is first demonstrated in Figure 6, Compared to the original image, the encrypted become noise-like images and are all actually unintelligible. Therefore, the proposed scheme indeed possessed high perceptual security.

(a) (a)Original Images (Fingerprints Embedding with 1-Level DWT), (b) (b) Original Images (Fingerprints Embedding with 2-Level DWT), (c) (c) Original Images (Fingerprints Embedding with 3-Level DWT)

Figure 5. Six Standard 512×512-Pixel Gray Scale Images with Fingerprints Embedding in DWT Domain

4.2. Imperceptibility of the Fingerprint

The fingerprint is embedded in the image before permutation and diffusion process. In order to preserve visual quality, the fingerprint in the fingerprinted copy should be imperceptible and perceptually undetectable. Figure 3, shows some experimental results of decrypted fingerprinted images (d). It can be observed that the quality of the fingerprinted image do not have any change.

4.3. Encryption Process

A good image encryption scheme needs to contain sufficiently large key space, and thus can effectively prevent invaders decrypting original data even after they invest large amounts of time and resources. The analysis results regarding the key space are summarized as follows. The key space consists of two pairs of the control parameters a, b and two pairs of the initial conditions x_0, y_0 in both processes, the four initial conditions are real numbers with 52-bit double precision. Therefore, the key space is about 2^{209}. A sufficient security against brute-force attacks with the proposed scheme can be provided. In addition, because the permutation process and the diffusion process are independent, the pirate still cannot decrypt the image even if the chaotic map used in permutation is cracked. Figure 6 shows the experimental results.

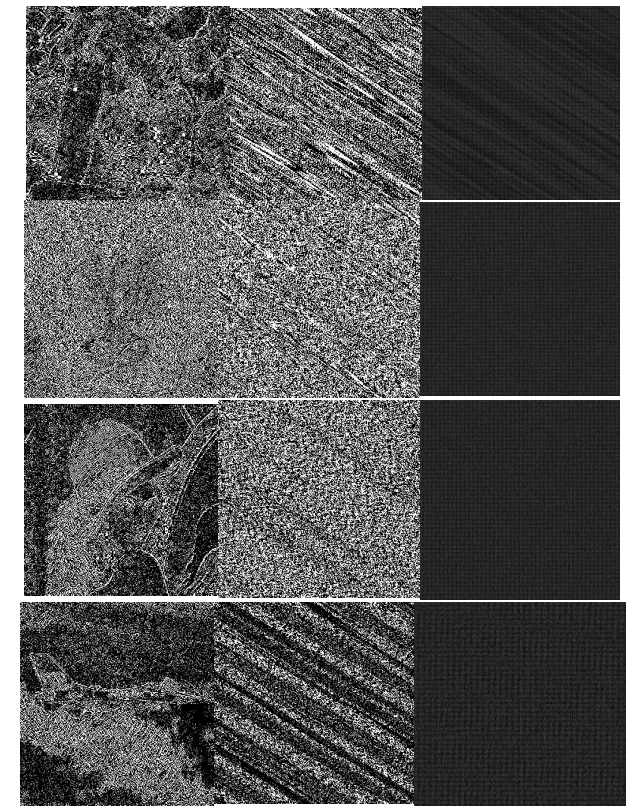

Figure 6. Content Encryption

5. Conclusion

In the proposed JFE scheme, we proposed an encryption process with multi chaotic maps, so the sufficiently large key space can effectively prevent invaders decrypting original data even after they invest large amounts of time and resources. For traitor tracing, the proposed JFE method can trace the illegal distribution. Theory analysis and experimental results prove that the proposed scheme is more efficient than the traditional unicast distribution mode. The proposed scheme is simple and easy to realize. By using our technique, one is well able to design a privacy-preserving and secure multimedia distribution system in M2M environment. By using the proposed scheme, three properties of multimedia content transmission can be ensured, including the distribution efficiency, privacy preserving and traitor tracing, which sometimes deter pirated behaviors. For the future work, we will analyze the security of joint fingerprinting and encryption scheme theoretically according to resource-constrained M2M communication environment.

Acknowledgments

This work is supported by the NSF of China under Grant No. 61502154, 61370092 and 61370223, Natural Science Foundation of Hubei Province of China (No. 2015CFB236, 2014CFB188), and Youth innovation team project in Hubei Provincial Department of Education (No. T201410).

Reference

[1] H. Liu, X. Wang, "Color image encryption based on one-time keys and robust chaotic maps", Comput. Math. Appl., 59 **(2010),** pp. 3320-3327.
[2] K. Chang, A. Soong, M. Tseng, Z. Xiang, "Global Wireless Machine-to-Machine Standardization", Internet Computing, IEEE, 15 **(2011)**, pp. 64-69.
[3] D.A. Bailey, "Moving 2 Mishap: M2M's Impact on Privacy and Safety", Security & Privacy, IEEE, 10 **(2012)**, pp. 84-87.
[4] R. Lu, X. Li, X. Liang, X. Shen, X. Lin, "GRS: The green, reliability, and security of emerging machine to machine communications", Communications Magazine, IEEE, 49 **(2011)**, pp. 28-35.
[5] G. Lawton, "Machine-to-machine technology gears up for growth", Computer, 37 **(2004)**, pp. 12-15.
[6] G. Chang, "A Survey on Security Issues of M2M Communications in Cyber-Physical Systems", KSII Transactions on Internet and Information Systems (TIIS), 6 (2012) 24-45.
[7] I. Cha, Y. Shah, A.U. Schmidt, A. Leicher, M. Meyerstein, "Trust in M2M communication", Vehicular Technology Magazine, IEEE, 4 (2009) 69-75.
[8] Pandey, M.J. Choi, M.S. Kim, J.W. Hong, "Towards management of machine to machine networks", in, IEEE, 2011, pp. 1-7.
[9] C. Hongsong, F. Zhongchuan, Z. Dongyan, "Security and Trust Research in M2M System".
[10] A. Bartoli, J. Hernández-Serrano, M. Soriano, M. Dohler, A. Kountouris, D. Barthel, Secure Lossless Aggregation Over Fading and Shadowing Channels for Smart Grid M2M Networks, Smart Grid, IEEE Transactions on, 2 **(2011)**, pp. 844-864.
[11] E. Barnhart, C. Bokath, Considerations for Machine-to-Machine communications architecture and security standardization, in, IEEE, **(2011)**, pp. 1-6.
[12] M. Saedy, V. Mojtahed, Ad Hoc M2M communications and security based on 4G cellular system, in, IEEE, **(2011)**, pp. 1-5.
[13] C.C. Chiu, S.Y. Chien, C. Lee, V.S. Somayazulu, Y.K. Chen, "Distributed video coding: A promising solution for distributed wireless video sensors or not?", in, IEEE, 2011, pp. 1-4.
[14] E. Lin, A.M. Eskicioglu, R.L. Lagendijk, E.J. Delp, Advances in digital video content protection, Proceedings of the Ieee, 93 **(2005)**, 171-183.
[15] D. Kundur, K. Karthik, "Video fingerprinting and encryption principles for digital rights management, Proceedings of the IEEE", 92 **(2004)**, pp. 918-932.
[16] C. Ye, J. Li, Z. Xiong, "Traceable Content Distribution Using Wavelet Decomposition and Social Network Analysis, in: Computer, Consumer and Control (IS3C)", 2012 International Symposium on, IEEE, **(2012)**, pp. 789-792.
[17] C. Ye, Z. Xiong, Y. Ding, G. Wang, J. Li, K. Zhang, "Joint fingerprinting and encryption in hybrid domains for multimedia sharing in social networks", Journal of Visual Languages & Computing, **(2014)**.

[18] C. Ye, Z. Xiong, Y. Ding, X. Zhang, G. Wang, F. Xu, "Joint Fingerprinting/Encryption for Medical Image Security", International Journal of Security and Its Applications, 9 **(2015)**, pp. 409-418.
[19] C.C. Chen, "A Verifiable and Traceable Secondhand Digital Media Market Protocol", KSII Transactions on Internet and Information Systems (TIIS), 5 **(2011)**, pp. 1472-1491.

Authors

Conghuan Ye received the B.S. and M.S. degree in computer science from Hubei Normal University, Hubei, China, in 2002, and University of Electronic Science and Technology of China, Chengdu, Sichuan, China, in 2005, respectively. Now, his research interests include digital fingerprinting, digital right management, complex network, and cloud computing. Dr.Ye received the scholarship from UESTC from 2003 to 2004.

Dr. Ye has co-authored over 30 publications including book chapters, journal and conference papers. He received the Ph.D. degree in computer science and technology, Huazhong University of Science and Technology (HUST) in 2013, Wuhan, Hubei, China. Since 2013, he has been an associate professor with the college of computer science and technology, HBEU.

Zenggang Xiong received the MA degree from Hubei University, China, in 2005, and the PhD degree in computer science from Beijing University of Science and Technology, China, in 2009. He is now a professor in Hubei Engineering University. His research interests are in the areas of peer-to-peer computing, Cloud computing, distributed systems and big data.

Yaoming Ding received the MA degree from Huazhong Normal University, China, in 2000, and the PhD degree in education from Huazhong Normal University, China, in 2011. He is now a professor in Hubei Engineering University. His research interests are in the areas of optical communication technology and cloud computing.

Xuemin Zhang received the Bachelor degree in computer science from Hubei Normal University, China, in 2001, and the MA degree in computer science from Wuhan University of Technology, China, in 2009. She is now an associate professor in Hubei Engineering University. Her research interests are in the areas of Cloud computing, distributed systems, Service Computing. She is a member of the IEEE and the ACM.

Guangwei Wang received the B.S. and M.S. degree in computer science from Huazhong Normal University, Wuhan, China, in 2005 and 2008, respectively. He received the Ph.D. degree from Huazhong University of Science and Technology in 2012. Now, He works in School of Computer and Information Science, Hubei Engineering University and his research interests include Computer vision and video analysis. He has co-authored more than 10 papers published in various journals.

Fang Xu received the B.S. and M.S. degree in computer science from Hubei Engineering University, Hubei, China, in 2003, and Wuhan University, Wuhan, Hubei, China, in 2009, respectively. Now, his research interests include Mobile Social Networks, digital fingerprinting, Machine Learning, and cloud computing.

Dr. Xu has co-authored over 20 publications including journal and conference papers. He is currently a Ph.D. student in the Wuhan University at Wuhan, majoring in computer science and technology.

